

Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121.

Listing of Claims:

1. (Currently amended) A record carrier ~~(1)~~ having a first area ~~(3)~~ storing information (data), which is at least partly stored in encrypted form (EAK(data)), this part being called an asset (EAK(data)), and which includes a first part of decryption information (HCK, EDNK(HCK)), and the record carrier ~~(1)~~ further having a second area ~~(4)~~ storing a second part of decryption information (UCID), wherein both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the asset (EAK(data));

wherein the first area comprises a storage medium of one physical kind and the second area comprises a storage medium of another physical kind.

2. (Cancelled)

3. (Currently amended) A record carrier ~~(1)~~ as claimed in claim 1, having a first area storing information (data), which is at least partly stored in encrypted form (EAK(data)), this part being called an asset (EAK(data)), and which includes a first part of decryption information (HCK, EDNK(HCK)), and the record carrier further having a second area storing a second part of decryption information (UCID), wherein both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the asset (EAK(data)); characterized in that wherein

the second area ~~(4)~~ comprises a chip ~~(4')~~ for providing the store of the second area ~~(4)~~.

4. (Currently amended) A record carrier ~~(1)~~ as claimed in claim 1, characterized in that wherein

a symmetric method using a first cryptographic key, called an asset key (AK), is used for asset ~~en-encryption~~ and decryption, and ~~in that~~

the asset key (AK) is stored in the second area (4) in an encrypted form, wherein for its encryption a symmetric encryption method has been used, this method employing a second cryptographic key (CIDK) in whose derivation both the first (HCK) and second (UCID) parts of decryption information have been used.

5. (Currently amended) A record carrier (1) as claimed in claim 1, characterized ~~in that wherein~~

a third cryptographic key, called a hidden-channel key (HCK), serves in the asset decryption, and ~~in that~~

the hidden-channel key (HCK) is obtainable from the first part of decryption information (HCK, EDNK(HCK)), ~~in particular, that the hidden-channel key (HCK) coincides with the first part of decryption information (HCK), and that the first part of decryption information (HCK) is scrambled and/or encrypted within the information (data) stored in the first area (3).~~

6. (Currently amended) A record carrier (1) as claimed in claim 3, characterized ~~in that wherein~~

the chip (4) is designed for storing a first counter (Ci), and

the chip (4) is designed for allowing ~~en-a~~ reading and/or writing device read access to the first counter (Ci) but denying write access to it, and

the chip (4) is designed for changing the value of the first counter (Ci) each time the second part of decryption information (UCID) is read by ~~en-the~~ reading and/or writing device, and

the chip (4) is designed for storing a second counter (Ce) in an encrypted form, wherein both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the second counter (Ce); and

~~wherein the payload data EAK(data) is decrypted if the second counter (Ce) coincides with the first counter (Ci).~~

7. (Currently amended) A record carrier $\langle 1 \rangle$ as claimed in claim 3, characterized in that wherein

the chip $\langle 4 \rangle$ is designed for checking the right of ~~an~~ a reading and/or writing device to access the record carrier $\langle 1 \rangle$.

8. (Currently amended) A record carrier $\langle 1 \rangle$ as claimed in claim 1, characterized in that wherein

the second area $\langle 4 \rangle$ is designed for storing user-specific settings serving in controlling the access of ~~an~~ a reading and/or writing device to the record carrier $\langle 1 \rangle$ and/or in controlling the manner information being read from the record carrier $\langle 1 \rangle$ is presented by the reading and/or writing device to a user of the reading and/or writing device.

9. (Currently amended) A device for reading from and/or writing to a record carrier $\langle 1 \rangle$ as claimed in claim 1, wherein the device is designed

for reading and/or writing the first part of decryption information (HCK, EDNK(HCK)),

for reading and/or writing the second part of decryption information (UCID), and for reading and/or writing the asset (EAK(data));

optionally, for obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information; and,

optionally, for decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information.

10. (Currently amended) A device for reading and/or writing as claimed in claim 9, characterized in that wherein

the device is designed for accessing the first $\langle 3 \rangle$ and second areas $\langle 4 \rangle$ of the record carrier $\langle 1 \rangle$ in parallel.

11. (Currently amended) A device for reading and/or writing as claimed in claim 9, characterized in that wherein

the device is designed for storing and maintaining a revocation list of identifiers (UCID), and ~~in that~~

~~the device is designed for at least partly refusing a user of the a device access to a record carrier (1) as claimed in claim 3 if the identifier (UCID) being stored on the record carrier (1) belongs to the revocation list.~~

12. (Cancelled)

13. (Currently amended) A method for reading from and/or writing to a record carrier (1) as claimed in claim 1, ~~with the steps comprising:~~

reading and/or writing the first part of decryption information (HCK, EDNK(HCK)), reading and/or writing the second part of decryption information (UCID), ~~and~~ reading and/or writing the asset (EAK(data)),

~~optionally, obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and,~~

~~optionally, decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information.~~

14. (Currently amended) A method for producing a record carrier (1) as claimed in claim 1, ~~with the steps further comprising:~~

~~selecting an identifier (UCID), in particular, selecting an identifier (UCID) being different from the identifiers (UCID) having previously been selected in the method,~~

~~constructing the second part of decryption information (UCID) as comprising the identifier (UCID), and~~

~~producing the record carrier (1) with the thus constructed second part of decryption information (UCID) being stored on the second area (4) of the record carrier (1).~~

15. (New) The device of claim 9, wherein the device is further designed for obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and

for decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information.

16. (New) The method of claim 13, further comprising:
obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and,
decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information.